18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

Quality of Information Approach to Improving Source Selection in Tactical Networks

Kevin Chan, Kelvin Marcus, Lisa Scott, Rommie Hardy
US Army Research Laboratory
Adelphi, MD 20783

***Abstract*—Intelligence operations in highly dynamic and constrained networked environments require a prudent strategies to query information sources. We consider the performance of this process based on metrics relating to quality of information: accuracy, timeliness, completeness and reliability. These metrics are identified in military doctrine as requirements that promote mission success. Further, it is possible to identify specific network metrics that are indicators of that the network is meeting these quality requirements. We study effective data rate, social distance, link integrity and the utility of information as metrics within a multi-genre network to determine the quality of information of its available sources. This paper proposes a formulation of the analytic hierarchy process to score information sources based on these concepts. A modification to this algorithm is also presented which incorporates the dynamics of the measurements. This is a multimodal fusion approach that considers elements from communications, information and social networks to assist a decision maker in the source selection problem. We show how this approach can be used to score information sources for such tasks using results from representative simulations.**

I. Introduction

Gathering intelligence in tactical networked environments is growing in complexity, particularly where the variety of available sources and methods to acquire information are continuously evolving and increasing. Intelligence analysts are required to make difficult decisions on which sources to pull information, based on the strict requirements of the mission. Available resources and capabilities will be far less than what is required to gather and process all of the available information. So analysts must make prudent choices from which sources to pull information. We consider a multimodal fusion approach to the selection of sources of information using elements of the complex tactical network environment. Additionally, the dynamics of the environment introduce uncertainty into the measurement validity affecting the trust in the fused information. In this paper, we fit the source selection problem in intelligence operations into the analytic hierarchy process (AHP) [1], handling the dynamics of the environment by accounting for the uncertainty in the measurements.

The source selection problem is not unique to tactical intelligence environments, where individuals must select information sources on a daily basis [2]. Individuals decide which websites or social network platforms to gather information on current events and personal interests. Most of this is done by inherent learning of preferences. For the tactical domain, the unique constraints and extreme requirements coupled with the constraints of an intelligence gathering operation require a methodical approach to source selection that is not as crucial in other domains.

First, the tactical network presents resource constraints on the network operators and the devices with which they are conducting intelligence operations. Additionally, these networks are operating within a disconnected, intermittent, low-bandwidth (DIL) environment [3]. However, there are strict mission requirements that perhaps are beyond the obvious capabilities of these networks. Joint Intelligence JP-2.0 states that *"careful consideration must be given to having multiple collection sources performing redundant collection, as collection requirements will usually exceed collection, processing, and exploitation capacity."* This work focuses on the constraint that the collection capacity is surpassed by the collection requirement for various tasks.

Second, the tactical network environment has increased in scope to consider beyond the net-centric warfare approach of traditional information assets. Network designers and operators have to conduct hard/soft information fusion [4] to incorporate various human intelligence (e.g., coalition partners, nongovernmental organizations and local civilians) with traditional hard assets in which trust and uncertainty with these sources is variable.

Third, the network monitoring problem is greatly impacted by the dynamics of the environment [5]. The state of the environment cannot be constantly assessed, so there is a great amount of uncertainty within the infor-

978-0-9964527-1-7

mation channels, particularly with regard to the freshness and accuracy of the network measurements. Gaining greater understanding of these network measurements requires additional time and communication overhead, which may be prohibitive in these tactical environments.

As a result, decision making within these situations is done with a significant amount of uncertainty. In this work, we are considering a multimodal fusion approach, where it will be valuable to understand how much this fused information and measurements can be trusted.

Various military doctrine establishes quality requirements for intelligence tasks. ADRP 2-0: Intelligence [6] and FM 7-15: The Army Universal Task List [7] provide evaluation techniques for gathered information from sources. Army Tactical Task, ART 7.2.1.3 [7], lists the assessment of collecting information in Table I, describing the relevant requirements for this work (requirements not in scope of this paper were omitted).

No.	Scale	Measure
01	Yes/No	Relevant information that meets the quality criteria serves the commander's needs
02	Time	To conduct assessment of collected relevant data
03	Percent	Of available information examined and considered in latest status reporting
04	Percent	Accuracy of data transmitted/disseminated
05	Percent	Of time information passed within established time criteria
06	Percent	Of time information on CCIR passed within established time criteria
07	Percent	Of time mission-essential intelligence and threat assessments passed within established time criteria
09	Percent	Of reports with no significant errors

TABLE I
EXCERPT FROM QUALITY OF INFORMATION RELATED REQUIREMENTS FROM ARMY TECHNICAL TASK 7.2.1.3

While the quality requirements are established, a standard operating procedure has not been established for such scenarios. In this paper, we use the Analytic Hierarchy Process (AHP) to provide a method to evaluate source qualities based on these metrics. Additionally, we consider dynamics and properties of this multi-genre network operating in a tactical environment. This discounting enables us to assess our trust in the AHP score, allowing commanders to have increased understanding of the accuracy of the process.

The contribution of this paper is the application of AHP to the QoI problem through the construction of the AHP hierarchy with regard to QoI and multi-genre network metrics. Additionally, we formulate a notion of trust based on the uncertainty of the network measurements caused by the dynamics of the environment. We show how uncertainty impacts the QoI score acquired by AHP. In the next section, we describe the various concepts involved in this work: quality of information, trust, and multimodal fusion. Then in Section IV, we adapt the AHP formulation to the source selection problem. Then, we show numerical examples of the formulation applied to two sample scenarios showing the fusion of multimodal network metrics from simulated and experimental data.

Through a characterization of the quality and trustworthiness of sources in the network, the rate of information flow to networked decision makers will be vastly improved. Our evaluation of the dynamics of information flows here is through characteristics relating to quality of information. We present a multimodal fusion approach to improve quality of information performance in a tactical network environment. Through the classification of various qualities of nodes within the network, process in which nodes are selected to provide information can be enhanced. This approach is also tunable according to the quality of information mission requirements.

II. BACKGROUND

As stated previously, the source selection problem has applications in various domains. Here, we focus on the tactical domain. This work is also seen as a multi-agent filtering problem [2], [8]. The idea of fusion with regard to trust has been explored in various contexts. Kaplan et al. [9] consider the concept of trust through the consistency of information from multiple sources to derive opinions through the fusion of information. Also, [10] initializes this paper by proposing an AHP formulation for the QoI problem. We extend this by proposing various connections to the multi-genre network properties and also incorporating trust and uncertainty into the scoring mechanism. In addition to the concept of fusion, this paper includes several other concepts which we briefly describe in the rest of this section.

Quality of Information (QoI) has been a recent concept within tactical military networks, assessing the quality of the content of the data along with the presentation of the data. There are many definitions of QoI, with content and scenario specific relevance to these dimensions. For information sharing and gathering scenarios, there is relevant work studying the content of the information. Military doctrine identifies QoI requirements and dimensions for for intelligence gathering [7], [6]. The quality metrics identified are accuracy, timeliness, completeness, precision, and reliability. Bar-Noy et al. [11] stress the stakeholder performance rather than simple communication networks metrics such as bandwidth and throughput. Here, they propose attributes of the information such as the source of information,

freshness, precision, and provenance. Bisdikian et al. [10] propose an ontology for QoI and the Value of Information (VoI), also proposing an AHP solution to the ontology. Here their attribute subcategories are relevance, integrity and timeliness. In this work, we consider further study with network metrics as subgoals for each of the QoI attributes.

Tactical network environments are comprised of intricate and dynamic relationships involving social, information and communications networks [12]. We represent the tactical environment as a multi-genre network, which includes elements of the tactical network space in scope greater than the military assets within a tactical environment. Given recent developments within network science research, we model the tactical network environment with a multi-genre network assuming that there are aspects of each of these constituent networks that impact our tactical scenario.

An accepted definition of trust is the willingness to accept a risk, while other definitions portray trust willingness to delegate authority. There are also obvious connections to trust in automation, given the process of delegating authority to another entity to provide information [13]. The version of trust that applies to the source selection problem in the tactical environment context is the willingness to trust fused information with variable freshness. It is the willingness to risk a decision based on the available measurements and associated uncertainty [14].

III. Problem Formulation

We assume a tactical scenario that a networked set of entities are deployed to conduct missions of various quality requirements. To perform these missions, the networked analyst is tasked with gathering intelligence from various information sources. The tactical network environment is severely constrained, highly dynamic and operating in the presence of a persistent adversary as discussed in the previous section.

The scenario assumes that an intelligence analyst constructed by a commander or decision maker that has variable access to a set of sources to conduct an intelligence gathering task. The analyst has a task that has specific QoI requirements and preferences between pairs of QoI requirements. Further, the analyst has access to a set of measurements for a set of network metrics taken with variable frequency. Each of the information sources is accessible to the analyst through a tactical military environment modeled by a multi-genre network. The source, if queried, provides information relevant to the query. We consider a sample intelligence scenarios that require data collection from information sources. We describe the scenario here and then provide AHP scoring for the scenario for several example sources in Section VI.

The intelligence scenario is an abstraction of a more operationalized environment. The Multi-Genre Network Science experiment conducted in [15] to determine the impact network science technologies have on communications network performance. Within the scenario, multiple remote sources are queried to retrieve data regarding a High Value Target (HVT) and his known associates. The query traverses an emulated tactical network where source nodes respond to the query and transcode the response data accordingly based upon the monitored network state (bandwidth and latency). The scenario is ultimately based upon field experiments performed by the Technical Support Operational Analysis (TSOA) at Camp Roberts and Multilevel Strategy (MLS) Scenario Modules developed by the Army's Training and Doctrine Command (TRADOC) [16]. In this scenario, timeliness supersedes the other quality requirements.

We assume that the communication network is a MANET, with limited bandwidth, communications range, so the end-to-end routes can be multi-hop. In the representation of the communications network [15], we use an emulation capability CORE/EMANE. Additionally, terrain and mobility effects can be represented. An additional property within the communication network is the security of the communication links being employed. Given the wireless network, keys used to encrypt traffic may be compromised; this measure of security is based on the level of hostility and security posture of the key management scheme.

The information network is assumed to be overlaid on the communications network, where information sources are receiving information from (hard or soft) sensors, that will send information back to the commander if asked to provide information. In this work, we use data from a command and control experimental platform called ELICIT, which allows agents or people to conduct an intelligence task within an organization. Sources provide information of varying value to the task, with potential application of requirements 5,6,7 in Table I. In this paper, we assume 3 levels of information value.

The assumption about the social network is that the analysts will be communicating with and through various echelons of the military organization. As a result, the pull of information may traverse through several levels (or even outside the military hierarchy) before reaching the analyst.

IV. AHP Criteria

We now propose the AHP hierarchy for the source selection problem. We describe the hierarchy, the QoI

criteria, and then the network metrics, with the relationships and dependencies shown in Figure 1.

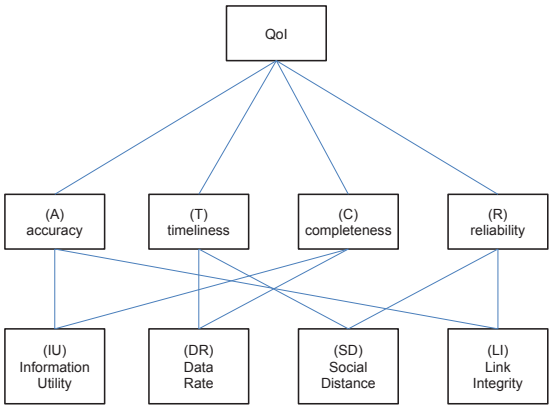

Fig. 1. Analytic Hierarchy Process hierarchy with QoI criteria and network metrics

A. QoI Metrics

We characterize QoI by the following metrics for this scenario: Accuracy (A), Timeliness (T), Reliability (R), and Competence (C), which is a subset of those identified in [7]. These are measurements of the behavior of the information sources with respect to the analysts.

Accuracy (A) is the correctness of the information of the source, whether it is relevant to accomplishing the task. This measure can also include if the information contains any conflicting or wrong information. In our model, accuracy measures if the information received provides correct information to achieve the task and the ability of the mission to be completed successfully.

Timeliness (T) is a measure of the ability of the source to provide information within the time requirement of the query. A stated in [7], the quality measure indicates how much information, information on Commander's Critical Information Requirements (CCIR), and mission-essential intelligence are received within the time criteria. Our approach models timeliness by the rate at which the analyst receives information, dependent on the communications links and the intermediate entities in the network.

Reliability (R) is a measure of the willingness of the source to be available to provide information when requests are made. This may also include the reliability of the data provided. As a result, this may also include the trustworthiness and integrity of the information provided.

Completeness (C) is the measure of the ability of the information provided to satisfy the tasks of the mission. This addresses the amount of critical information that has been received by the commander by the time requirements, as described in [7].

B. Network Metrics

Our model uses the following network metrics to define QoI criteria: effective data rate (DR), utility of information (UI), link integrity (LI), and social distance (SD). These are metrics from multi-genre networks that reside in one of the network layers, social, communications and information. We briefly describe the network metrics and the dynamics of the measurement. While the data that is used has not been gathered from the same experiments, the data we provide is an example of a potential tactical scenario and could represent the behavior of a node in a single experiment; where further investigation requires a unified experiment platform and better understanding of the complex relationships of these metrics.

Data rate (DR): In terms of impact to the QoI metrics, bandwidth will directly impact timeliness and completeness. The data rate determines how much and how quickly information is sent to the analyst. Data to represent this metric has been gathered by running an EMANE scenario composed of heterogeneous communication nodes with varying CPU and RAM, varying application sets with varying behavior. Furthermore each node is geographically dispersed throughout a hybrid network composed of multi-tiered mobile ad hoc, cellular and fixed networks, all factors that can affect bandwidth/data rate dynamics [15]. The experiment conducted in[15] provided a source for realistic troop movement patterns, network topologies and bandwidth/data rates. An example realized data rate from three sources is shown in Figure 2(UL), where the bandwidth is set to 1 Mbps and the effective data rate is measured every 2 seconds. The data rate network metric is normalized to have 1 represent 1 Mbps.

Utility of Information (UI): In intelligence tasks, a general model of the process is that the information sources are sensing some environmental entity or action, storing this raw information of the observation, and then sending it to the analyst when requested. The accuracy and completeness of the information are determined by the capability of the source and sensor, and also the environmental conditions. In addition to the communications range of such nodes in a MANET, we can also assume that there is an effective sensing range of these sensors.

For our model, the data has an objective value to the analyst. Information factoids f, as ELICIT calls them, will have one of three values, which can be an abstraction to the ART defined in Table I in terms of information, CCIR information and mission critical information being

passed. This would represent a scaling of the effective value of the information factoids. The utility of the information received by source i is defined by

$$UI_i(t) = \alpha_1 f_1(t) + \alpha_2 f_1(t) + \alpha_3 f_3(t) \quad (1)$$

where $\{\alpha_1, \alpha_2, \alpha_3\}$ are weights for the information value in decreasing value. For our simulations, we use the values $\{.70, .25, .05\}$. The number of factoids of each value sent by source i are $f_1(t), f_2(t), f_3(t)$. Measurements are taken every 3 minutes as is evaluated by the factoids received in that period of time.

Social distance (SD): Social distance impacts QoI by the number of entities through which the analysts must communicate to receive information. Different than hop count in a multi-hop communication network, this is the analog for the social network. By having to communicate through multiple entities, this affects the timeliness of the received information. Further, the multi-hop communications through potentially less trustworthy sources or forwarders of information will influence the reliability of the information received. As an abstraction to the military force structure for intelligence operations, we assume a maximum distance of 4 hops. Also synthetic measurements were generated every 4 minutes. Fig. 2(UR) shows the social distance for the three example sources.

Link Integrity (LI): QoI definitions do not explicitly address the security of the information, but the integrity of the links will have significant impact on the accuracy and reliability of information sourced from paths containing compromised links. Security in MANETs can employ a key predistribution schemes to protect against node and key compromises. While other schemes can be used, we use approaches from [17], [18] to simulate the effective link security of paths from the information source to the analyst. In this paper, LI is drawn from a simulation 100 nodes randomly deployed with a set of 20 keys drawn randomly from a pool consisting of 362 unique keys. Secure links are established if two nodes within communication range have at least one key in common. Links can become compromised or vulnerable from different adversarial mechanisms therefore, associating a measure of link integrity. According to [17], the vulnerability of a link can be measured by its resilience to key compromise. In a network where keys are used to encrypt communications links, keys can be added and revoked as part of periodic updates, or in response to network events such as new nodes leaving or joining the network. Link vulnerability can be combined with link metrics in order to determine routes within a network thus altering the flow of information. Node captures occur, signaling that a random set of nodes and their keys

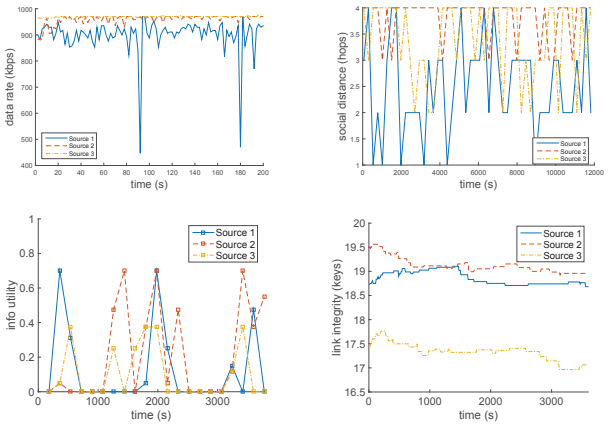

Fig. 2. Network Metrics for three example nodes, (UL) Data Rate - DR, (UR) Social Distance - SD, (LL) Information Utility - IU, (LR) Link Integrity - LI.

were compromised by the adversary. A link is considered compromised if all the keys that make up that links have become compromised. Therefore, the vulnerability of a link $\ell(i,j)$ based upon its key distribution can be determined by the following

$$\ell(i,j) = \sum_{S \in \mathcal{K}_{ij}} \frac{(-1)^{|S|+1} N}{|N_S|} \quad (2)$$

The above equation can be used to measure the associated integrity of a link based on said adversarial model. As a result, this behavior affects both reliability and accuracy of QoI performance. Three sample link integrity traces have been extracted to represent the behavior of three sources, shown in Fig. 2(LR).

V. AHP Formulation

We apply the analytic hierarchy process (AHP) to the source selection process, where the overall goal is to order the QoI score for all possible sources. The criteria are the QoI dimensions as described in IV-A: Accuracy (A), Timeliness (T), Completeness (C), Reliability (R). The sub-criteria are the network metrics as described in IV-B, data rate (DR), link integrity (LI), utility of information (UI), and social distance (SD).

The preferences for the criteria and sub-criteria are defined by the requirements of the scenario. This approach allows for a configurable (these parameters themselves can also be learned) classification step according to quality of information dimensions. This feature allows for this formulation to be mission-context specific. Additionally, this approach is attractive in that it is clear how other dimensions and criteria can be added.

Based on the requirements of the scenario, We make assumptions on the priorities for Scenario 1, reflecting

the timeliness priority. We use AHP to establish the weights for the QoI criteria, $w = [w_T, w_A, w_C, w_R]$ and the sub-criteria, for timeliness ($w_{T,DR}, w_{T,SD}$), accuracy ($w_{A,LI}, w_{A,UI}$), completeness ($w_{C,DR}, w_{C,UI}$), reliability ($w_{R,LI}, w_{R,SD}$).

Given that each network metric will be scored in the range $[0, 1]$, we construct the following heuristic to assign a pairwise evaluation for the AHP matrix of option scores. Denote the pairwise values AHP v_z assigns to be in the set by V. In the case of source selection, there may be a large number of options, so pairwise comparison may be prohibitive. We propose the following heuristic for pairwise scoring and comparison of sources, i and j, for each network metric. For i, j, let $\Delta s = s_k(i) - s_k(j)$. Also, let $v_x(i,j) = 1/v_x(j,i)$. For the event s_z, which corresponds to the (fractional) score given to that event, we assign the pairwise score for the AHP framework and the range of Δs,

$$v_k(i,j) = \begin{cases} s_{19} & \frac{1}{9} & & \Delta s & < -.7 \\ s_{17} & \frac{1}{7} & -.5 < & \Delta s & \leq -.7 \\ s_{15} & \frac{1}{5} & -.3 < & \Delta s & \leq -.5 \\ s_{13} & \frac{1}{3} & -.1 < & \Delta s & \leq -.3 \\ s_1 & 1 & & |\Delta s| & \leq .1 \\ s_3 & 3 & .1 < & \Delta s & \leq .3 \\ s_5 & 5 & .3 < & \Delta s & \leq .5 \\ s_7 & 7 & .5 < & \Delta s & \leq .7 \\ s_9 & 9 & .7 < & \Delta s & \end{cases} \quad (3)$$

Further, as measurements of each source are gathered, a distribution of measurement of metric k will be established, $Pr(\mathcal{X}_k = i)$. To account for this uncertainty, we also a scoring method of the comparisons of the network metrics as a function of the joint distribution of the pairs of network metric scores, $Pr(\mathcal{X}_k = i, \mathcal{X}_\ell = j)$ and the weights as specified in (3). We also assume that these measurements are independent. So for $s_k(i), s_k(j)$, the AHP-weighted score for network metric k for node i with respect to node j is

$$s_k(i,j) = \sum_{i,j} Pr(\mathcal{X}_k = i) Pr(\mathcal{X}_\ell = j) v_k(i,j) \quad (4)$$

With the following process, individuals scores for source i for network metric k can be found, $S_k(i)$ as well as the overall QoI scores $S(i)$ for all sources i using AHP. As the measurements are being taken with varying frequency, the AHP uses the most recent set of network metrics scores for each source.

An example of how the joint distribution of the measurements are used in the AHP is shown in Fig. 3. The regions for each AHP score are indicated in Fig. 3(L). An example joint distribution for $s_k(i)$ and $s_k(j)$ is shown in Fig. 3(C). The joint distribution is weighted by the AHP score regions in Fig. 3(R). Then, the value for source i for metric k (and $v_k(j,i) = 1/v_k(i,j)$) is obtained by,

$$v_x(i) = \sum_{z \in Z} p_x(i,z) v_z, \quad (5)$$

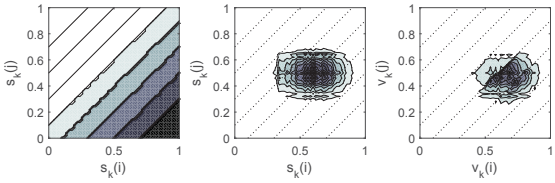

Fig. 3. Example scoring of $s_k(i)$ and $s_k(j)$ to obtain $v_k(i,j)$, with (L) indicating the nine regions of AHP scoring from (3), (C) showing joint distribution of i, j, and (R) showing the AHP-weighted joint distribution.

So, this method is a variant of the AHP with the consideration of uncertainty in the measurements of the criteria. For the source selection problem in the tactical environment, we can study the dynamics of the source selection as time progresses. As can be observed with the dynamics of the environment, it is not possible to fully characterize the quality of the information sources available. Therefore, we must account for the uncertainty and establish and estimate of the trust of these sources.

We now describe a proposed method to handle the uncertainty introduced by the dynamics of the environment and derive a trust score for each of the sources. As shown in Section IV-B, the estimates of the distributions of DR, SD, LI, UI vary over time and are learned over the course of limited observations. The dynamics of the tactical environment results in uncertainty in these measurements, so the history of the past observed behavior is considered. There are many methods to discount for freshness of data and other non-linear treatments of evidence, but for simplicity, we equally weight past evidence. Additionally, one can consider various approaches to initializing the distribution evidence [19]. The following section describes our approach to modeling the evaluation of trust based on the uncertainty resulting in evidence gathered from past experiences with various information sources.

For network measure k, the empirically obtained distribution will have variance $\sigma_k(t)$ at time t. We scale the uncertainty measure by the maximum variance ($\sigma_{max} = \frac{1}{4}$) the metric can exhibit for a random variable over [0,1]. For each source, we define trust $\tau_k(t)$ to be complement to the normalized uncertainty

$$\tau_k(t) = 1 - \frac{\sigma_k(t)}{\sigma_{max}} \quad (6)$$

Given the preferences of the QoI metrics obtained from AHP, we weight the individual trust scores by the

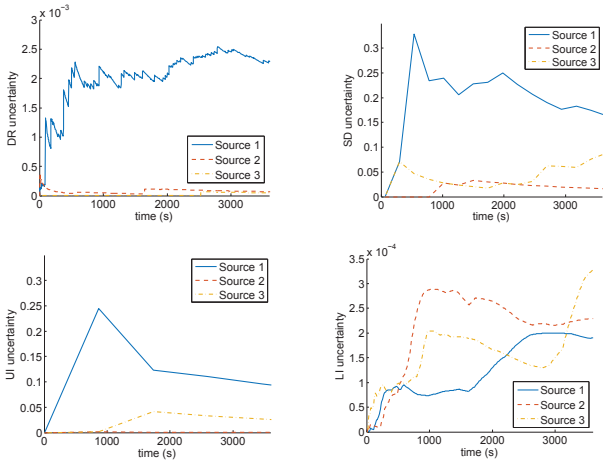

Fig. 4. Uncertainty of Network Metrics for three example nodes, (UL) Data Rate - DR, (UR) Social Distance - SD, (LL) Information Utility - IU, (LR) Link Integrity - LI.

AHP weights for the QoI values as is defined in (9) and obtain the trust of source i,

$$\mathcal{T}_i(t) = \sum_k w_k \tau_k(t) \tag{7}$$

While we do not combine the trust value into the AHP evaluation, the trust score can be used to assess confidence in the QoI score for particular sources. We note that this is distinct from the AHP consistency score, as that is relative to the other sources. We show the normalized uncertainty scores $\tau_k(t)$ for each of the QoI criteria in Fig. 4.

VI. Simulation

Based on the requirements of the scenario, we generate the following pairwise comparisons between T, A, C, R in (8).

$$AHP_1 = \begin{bmatrix} 1 & 3 & 7 & 7 \\ \frac{1}{3} & 1 & 5 & 3 \\ \frac{1}{7} & \frac{1}{5} & 1 & 7 \\ 1 & 3 & 7 & 1 \end{bmatrix} \tag{8}$$

which results in the following weights for the QoI criteria, w,

$$w = [w_T, w_A, w_C, w_R] = [.584, .251, .056, .109] \tag{9}$$

and the sub criteria where the relationships are defined in Fig. 1,

$$\begin{aligned} (w_{T,DR}, w_{T,SD}) &= (9/10, 1/10) \\ (w_{A,LI}, w_{A,UA}) &= (1/6, 5/6) \\ (w_{C,DR}, w_{C,UA}) &= (1/4, 3/4) \\ (w_{R,LI}, w_{R,SD}) &= (7/8, 1/8) \end{aligned}$$

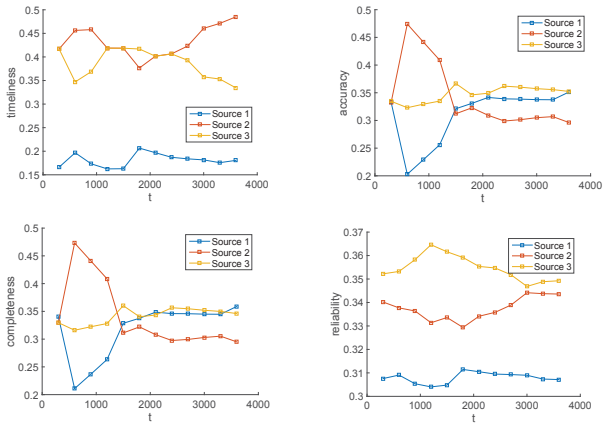

Fig. 5. QoI criteria scores for three sources based on AHP with (UL) Timeliness - T, (UR) Accuracy - A, (LL) Completeness - C, and (LR) Reliability - R.

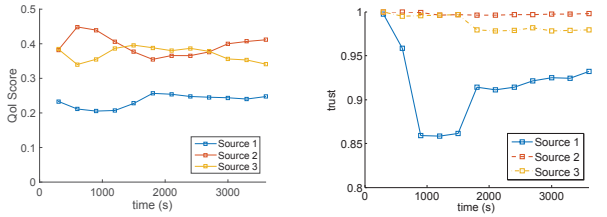

Fig. 6. QoI (L) and Trust (R) scores for the example scenario

Given the example source network measurements in Figure 2, we are able to obtain QoI score and trust scores for each of the three sources for the example scenario. Figure 5 shows the scores for each QoI criteria over the duration of the task. Additionally, Fig. 5 shows both the overall QoI score and trust score for the three sources.

When single parameters are chosen as the basis for decision-making, one can expect a less robust or more un-informed approach to selections in sources. Example of this is comparing the effective data rate to the QoI score. this is shown in Fig. 7. The running average of DR is shown, comparing that with the QoI score. One can see qualitatively, that the AHP approach ranking between Sources 2 and 3 are different 6 of the 13 scoring rounds. While we are unable to produce a ground truth as to which source selection approach is optimal. It is possible to understand that the AHP approach is considering other aspects of the multi-genre network which would make Source 2 more desirable to select over Source 3.

VII. Conclusion

In this paper, we proposed an initial AHP formulation for a source selection problem while considering QoI criteria. Additionally, we are able to account for the

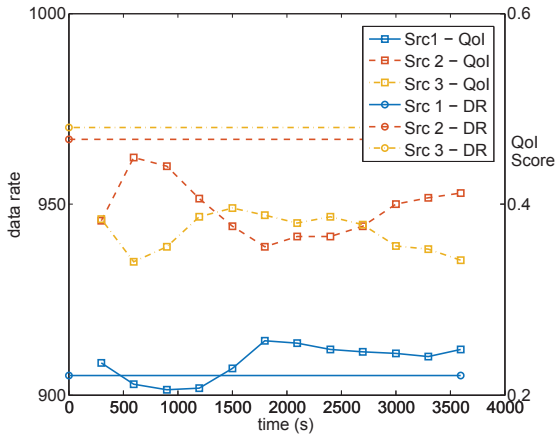

Fig. 7. QoI score vs. effective data rate ranking.

trust in the fused information by identifying uncertainty in the measurements. Through this approach, we are able to perform a multimodal fusion approach to identify sources which may provide the most QoI and an indication of the trust in the QoI scoring of sources in tactical network environments. We show a simple example of how this multimodal approach may enhance the decision-making process of analysts. This provides a methodical approach that is tunable to the requirements or the criteria of the task. Further, this provides an efficient method for analysts to perform source selection for intelligence tasks, which is crucial to stringent quality requirements asked of intelligence analysts.

REFERENCES

[1] T. Saaty, *The Analytic Hierarchy Process*. McGraw-Hill, 1980.

[2] D. M. S. Albayrak, "Situation-aware coordination in multi-agent filtering framework," in *Computer and Information Sciences - ISCIS 2004*, ser. Lecture Notes in Computer Science, 2004, vol. 3280, pp. 480–492.

[3] K. Scott, T. Refaei, N. Trivedi, J. Trinh, and J. Macker, "Robust communications for disconnected, intermittent, low-bandwidth (dil) environments," in *Military Communications Conference (MILCOM)*, Nov 2011, pp. 1009–1014.

[4] D. Hall, M. McNeese, J. Llinas, and T. Mullen, "A framework for dynamic hard/soft fusion," in *11th International Conference on Information Fusion*, June 2008, pp. 1–8.

[5] R. Hofstede and T. Fioreze, "Surfmap: A network monitoring tool based on the google maps API," in *IFIP/IEEE International Symposium on Integrated Network Management*, June 2009, pp. 676–690.

[6] *ADRP2-0: Intelligence*, United States Department of the Army, August 2012.

[7] *FM 7-15 C10: The Army Universal Task List*, United States Department of the Army, June 2012.

[8] R. Balakrishnan and S. Kambhampati, "SourceRank: Relevance and trust assessment for deep web sources based on inter-source agreement," in *Proceedings of the 19th International Conference on World Wide Web*, ser. WWW '10, 2010, pp. 1055–1056.

[9] L. Kaplan, M. Sensoy, and G. de Mel, "Trust estimation and fusion of uncertain information by exploiting consistency," in *2014 17th International Conference on Information Fusion (FUSION)*, July 2014.

[10] C. Bisdikian, L. M. Kaplan, and M. B. Srivastava, "On the quality and value of information in sensor networks," *ACM Trans. Sensor Networks*, vol. 9, no. 4, Jul. 2013.

[11] A. Bar-Noy, G. Cirincione, R. Govindan, S. Krishnamurthy, T. LaPorta, P. Mohapatra, M. Neely, and A. Yener, "Quality-of-information aware networking for tactical military networks," in *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, March 2011, pp. 2–7.

[12] P. Basu, R. Gibbens, T. La Porta, C.-Y. Lin, A. Swami, and E. Yoneki, "Guest editorial: Network science," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 993–996, June 2013.

[13] J. D. Lee and K. A. See, "Trust in automation: Designing for appropriate reliance," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 46, no. 1, pp. 50–80, 2004.

[14] I. Yaniv and E. Kleinberger, "Advice taking in decision making: Egocentric discounting and reputation formation," *Organizational Behavior and Human Decision Processes*, vol. 83, no. 2, pp. 260 – 281, 2000.

[15] K. Marcus, "Application of the dynamically allocated virtual clustering management system to emulated tactical network experimentation," in *Proc. SPIE 9079, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR V, 907904*, June 2014.

[16] United States Army Training and Doctrine Command. [Online]. Available: http://www.tradoc.army.mil/About.asp

[17] A. Clark and R. Poovendran, "A metric for quantifying key exposure vulnerability in wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, April 2010.

[18] A. Clark, R. Hardy, and R. Poovendran, "A joint performance-vulnerability metric framework for designing ad hoc routing protocols," in *In IEEE Military Communications Conference*, Nov 2010.

[19] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.